(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－271438
（P2003－271438A）
(43)公開日　平成15年９月26日(2003.9.26)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	12/00	537	G06F	12/00	537H　5B017
	12/14	320		12/14	320B　5B075
	17/30	120		17/30	120B　5B082
H04L	9/08		H04L	9/00	601B　5J104

審査請求　未請求　請求項の数６　ＯＬ　（全９頁）

(21)出願番号　特願2002－73047(P2002－73047)

(22)出願日　平成14年３月15日(2002.3.15)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号

(72)発明者　原嶋　秀次
東京都府中市東芝町１番地　株式会社東芝府中事業所内

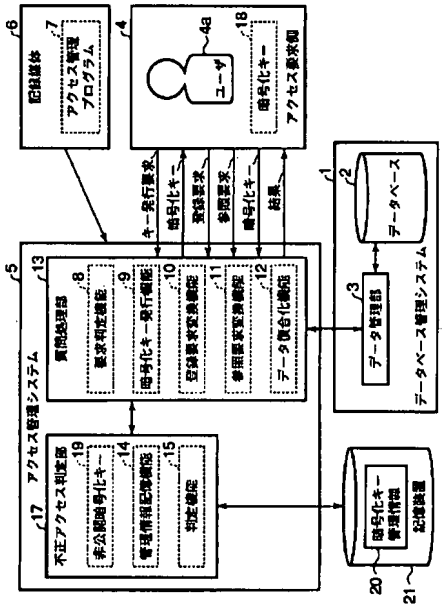
(72)発明者　駒津　公一
東京都府中市東芝町１番地　株式会社東芝府中事業所内

(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　アクセス管理プログラム及びシステム並びに方法

(57)【要約】
【課題】データベース管理者にデータベースの運用管理上必要なアクセス権限を認めつつ個々のデータの内容が把握されることを防止し、十分なデータ保護を実現する。
【解決手段】本発明では、アクセス要求側４に対して暗号化キー１８が発行され、暗号化キー１８とともに登録要求が受け付けられると、この暗号化キー１８を利用して暗号化されたデータがデータベース２に登録される。また、暗号化キー１８とともに参照要求が受け付けられると、この暗号化キー１８を利用してデータベース２に登録されている暗号化されたデータが参照され、参照されたデータが復号化される。



1

【特許請求の範囲】
【請求項１】　コンピュータに、アクセス要求側に対して暗号化キーを発行するキー発行機能と、
前記アクセス要求側からデータベースへの登録要求と前記アクセス要求側に発行された暗号化キーとを受け付け、前記アクセス要求側から受け付けた暗号化キーを利用して前記登録要求に含まれているデータを暗号化した変換後の登録要求を求め、前記変換後の登録要求を前記データベースに発する登録要求変換機能と、
前記アクセス要求側から前記データベースの参照要求と前記アクセス要求側に発行された暗号化キーとを受け付け、前記アクセス要求側から受け付けた暗号化キーを利用して前記参照要求に含まれているデータを暗号化した変換後の参照要求を求め、前記変換後の参照要求を前記データベースに発する参照要求変換機能とを実現させるためのアクセス管理プログラム。
【請求項２】　請求項１記載のアクセス管理プログラムにおいて、
コンピュータに、
前記変換後の参照要求に基づいて参照されたデータを前記アクセス要求側から受け付けた暗号化キーを利用して復号化し、この復号化されたデータを前記アクセス要求側に提供するデータ復号化機能を実現させるアクセス管理プログラム。
【請求項３】　請求項１又は請求項２記載のアクセス管理プログラムにおいて、
コンピュータに、
前記アクセス要求側に発行された暗号化キーを非公開の暗号化キーを利用して暗号化し、この暗号化された暗号化キーと前記アクセス要求側の識別情報とを関連付けて暗号化キー管理情報に登録する管理情報記憶機能と、
前記アクセス要求側から暗号化キーを受け付けた場合に、前記非公開の暗号化キーを利用して、前記暗号化キー管理情報に登録されており前記アクセス要求側を示す識別情報に関連付けされた情報と前記アクセス要求側から受け付けた暗号化キーとの一致性を判定し、一致性が認められない場合に前記アクセス要求側からのアクセスを禁止する判定機能とを実現させるアクセス管理プログラム。
【請求項４】　請求項３記載のアクセス管理プログラムにおいて、
前記判定機能は、一致性が認められないと判定された回数をカウントし、所定の回数以上となった場合に前記アクセス要求側からのアクセスを禁止するアクセス管理プログラム。
【請求項５】　データベースへのアクセスを管理するシステムにおいて、
アクセス要求側に対して暗号化キーを発行するキー発行手段と、
前記アクセス要求側からデータベースへの登録要求と前記アクセス要求側に発行された暗号化キーとを受け付け、前記アクセス要求側から受け付けた暗号化キーを利用して前記登録要求に含まれているデータを暗号化した変換後の登録要求を求め、前記変換後の登録要求を前記データベースに発する登録要求変換手段と、
前記アクセス要求側から前記データベースの参照要求と前記アクセス要求側に発行された暗号化キーとを受け付け、前記アクセス要求側から受け付けた暗号化キーを利用して前記参照要求に含まれているデータを暗号化した変換後の参照要求を求め、前記変換後の参照要求を前記データベースに発する参照要求変換手段とを具備したアクセス管理システム。
【請求項６】　コンピュータによりデータベースへのアクセスを管理する方法において、
アクセス要求側からデータベースへの登録要求と前記アクセス要求側に予め発行された暗号化キーとを受け付け、
前記アクセス要求側から受け付けた暗号化キーを利用して前記登録要求に含まれているデータを暗号化した変換後の登録要求を求め、前記変換後の登録要求を前記データベースに発し、
前記アクセス要求側から前記データベースの参照要求と前記アクセス要求側に発行された暗号化キーとを受け付け、
前記アクセス要求側から受け付けた暗号化キーを利用して前記参照要求に含まれているデータを暗号化した変換後の参照要求を求め、前記変換後の参照要求を前記データベースに発するとしたアクセス管理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータシステムにおいて各種データベース管理システム、ファイルシステムで管理されているデータへのアクセスを管理するプログラム及びシステム並びに方法に関する。
【０００２】
【従来の技術】リレーショナルデータベース管理システム（以下、「ＲＤＢＭＳ」という）やファイルシステムは、複数のユーザやアプリケーションがアクセス可能なデータソース（以下、「データベース」という）を管理する。
【０００３】ＲＤＢＭＳやファイルシステムは、ユーザ管理機能により、データベースへの不正なアクセスを防止している。例えば、ユーザ管理機能により、あるユーザに関するデータがアクセス権限のない他のユーザに参照されたり、書き換えられたりすることが防止される。
【０００４】
【発明が解決しようとする課題】しかしながら、一般的にデータベース管理者は、いずれのユーザに関するデータであってもアクセスする権限を有する。
【０００５】したがって、ユーザ管理機能を利用しても

データベース管理者がデータを漏洩することを防止することは困難である。

【0006】また、不正なユーザがデータベース管理者になりすましてデータベースをアクセスする場合もある。

【0007】本発明は、以上のような実情に鑑みてなされたもので、データベース管理者にデータベースの運用管理上必要なアクセス権限を認めつつ、個々のデータの内容が把握されることを防止し、十分なデータ保護を実現するアクセス管理プログラム及びシステム並びに方法を提供することを目的とする。

【0008】

【課題を解決するための手段】本発明を実現するにあたって講じた具体的手段について以下に説明する。

【0009】本発明のアクセス管理プログラムは、コンピュータに、アクセス要求側に対して暗号化キーを発行するキー発行機能と、アクセス要求側からデータベースへの登録要求とアクセス要求側に発行された暗号化キーとを受け付け、アクセス要求側から受け付けた暗号化キーを利用して登録要求に含まれているデータを暗号化した変換後の登録要求を求め、変換後の登録要求を前記データベースに発する登録要求変換機能とを実現させる。また、本発明のアクセス管理プログラムは、コンピュータに、アクセス要求側からデータベースの参照要求とアクセス要求側に発行された暗号化キーとを受け付け、アクセス要求側から受け付けた暗号化キーを利用して参照要求に含まれているデータを暗号化した変換後の参照要求を求め、変換後の参照要求をデータベースに発する参照要求変換機能を実現させる。

【0010】これにより、発行された暗号化キーによって暗号化されたデータがデータベースに登録されるため、データベース管理者や不正な他のユーザがデータベースのデータをアクセスした場合であってもそのデータの内容を把握・解読することができない。したがって、データベース管理者にデータベースの管理に必要なアクセス権限を認めつつ十分なデータ保護を実現することができる。

【0011】なお、本発明のアクセス管理プログラムは、コンピュータに、変換後の参照要求に基づいて参照されたデータをアクセス要求側から受け付けた暗号化キーを利用して復号化し、この復号化されたデータをアクセス要求側に提供するデータ復号化機能を実現させるとしてもよい。

【0012】また、本発明のアクセス管理プログラムは、コンピュータに、アクセス要求側に発行された暗号化キーを非公開の暗号化キーを利用して暗号化し、この暗号化された暗号化キーとアクセス要求側の識別情報とを関連付けて暗号化キー管理情報に登録する管理情報記憶機能と、アクセス要求側から暗号化キーを受け付けた場合に、非公開の暗号化キーを利用して、暗号化キー管理情報に登録されておりアクセス要求側を示す識別情報に関連付けされた情報とアクセス要求側から受け付けた暗号化キーとの一致性を判定し、一致性が認められない場合にアクセス要求側からのアクセスを禁止する判定機能とを実現させるとしてもよい。

【0013】これにより、不正なユーザが様々な暗号化キーを与え、暗号化されたデータの復号化を試みるような不正アクセスを防止できる。

【0014】また、判定機能は、一致性が認められないと判定された回数をカウントし、所定の回数以上となった場合にアクセス要求側からのアクセスを禁止するとしてもよい。

【0015】これにより、ある設定された回数を超えて一致しない暗号化キーを受け付けた場合に、アクセスを禁止することができる。

【0016】上記のようなアクセス管理プログラム、及びこのプログラムを記録した記録媒体を用いることによって、上述した機能を有していないコンピュータ、コンピュータシステム、サーバやクライアント等に対して、簡単に上述した機能を付加することができる。

【0017】本発明のアクセス管理プログラムで実現される機能と同様に動作する手段をアクセス管理システムに具備してもよい。

【0018】また、本発明のアクセス管理プログラムによって実施されるアクセス管理方法を発明の対象としてもよい。

【0019】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態について説明する。なお、以下に示す各図において、同一の部分については同一の符号を付してその説明を省略する。

【0020】（第1の実施の形態）本実施の形態においては、データベースに対して発せられる要求に含まれている機密事項のデータを暗号化し、データベース管理者や他のユーザ、他のアプリケーションがデータをアクセスしてもその内容を解釈できないようにする。

【0021】図1は、本実施の形態に係るアクセス管理プログラム及びアクセス管理システムの一例を示すブロック図である。

【0022】データベース管理システム1としては、データベース2を管理する一般的なシステムを適用可能である。データベース管理システム1のデータ管理部3は、例えば一般的なRDBMSなどに具備される質問処理部と同様の動作を行う。なお、このデータベース管理システム1は、オペレーティングシステムが提供するファイルシステムにアクセスインタフェースを付加したものであってもよい。

【0023】アクセス要求側4は、データベース2に対するデータ登録、データ参照（データの参照にはデータ検索も含むとする）などの要求を発する。アクセス要求

5

側4の具体例としては、ユーザ４ａ、データベース管理者、アプリケーション、外部システムなどがある。なお、本実施の形態においては、アクセス要求側４がユーザ４ａである場合について説明するが、他の場合でも同様である。

【００２４】アクセス管理システム５は、記録媒体６に記録されているアクセス管理プログラム７を読み込み、実行する。

【００２５】アクセス管理プログラム７は、アクセス管理システム５上で起動されると、要求判定機能８、暗号化キー発行機能９、登録要求変換機能１０、参照要求変換機能１１、データ復号化機能１２を実現する。これらの機能８～１２は、アクセス管理システム５の質問処理部１３に対応する。

【００２６】加えて、アクセス管理プログラム７は、アクセス管理システム５上で起動されると、管理情報記憶機能１４、判定機能１５を実現する。これらの機能１４、１５は、アクセス管理システム５の不正アクセス判定部１７に対応する。

【００２７】ユーザ４ａは、データベース２に対する登録要求をアクセス管理システム５に発する。登録要求は、機密事項のデータを含む。

【００２８】また、ユーザ４ａは、データベース２に対する参照要求をアクセス管理システム５に発する。参照要求には、参照条件が含まれている。

【００２９】そして、ユーザ４ａは、発した要求に対する結果をアクセス管理システム５から受ける。

【００３０】質問処理部１３は、ユーザ４ａからの要求に関る各種機能８～１２を実行する。

【００３１】要求判定機能８は、ユーザ４ａからの要求を受け付け、要求の種類を判定する。要求の種類には、主にキー発行要求、登録要求、参照要求などがある。

【００３２】暗号化キー発行機能９は、ユーザ４ａからキー発行要求を受け付けた場合に、ユーザ４ａに対する暗号化キー１８を生成し、ユーザ４ａに暗号化キー１８を発する。

【００３３】登録要求変換機能１０は、ユーザ４ａからの登録要求と暗号化キー１８とを受け付け、暗号化キー＊

6

＊１８を利用して登録要求に含まれている機密事項のデータを暗号化し、この暗号化されたデータを含む変換後の登録要求をデータベース管理システム１に発する。

【００３４】参照要求変換機能１１は、ユーザからの参照要求と暗号化キー１８とを受け付け、暗号化キー１８を利用して参照要求に含まれているデータを暗号化し、この暗号化されたデータを含む変換後の参照要求をデータベース管理システム１に発する。

【００３５】データ復号化機能１２は、変換後の参照要求に応じてデータベース２から読み出されたデータをデータベース管理システム１から受け付け、暗号化キー１８を利用して読み出されたデータを復号化し、参照結果としてユーザ４ａに提供する。

【００３６】不正アクセス判定部１７は、ユーザ４ａからのアクセスが不正か否かチェックし、不正なアクセスと判定した場合にこのアクセスを禁止する。不正アクセス判定部１７には、外部から読み取ることが不可能な状態で非公開暗号化キー１９が内蔵されている。

【００３７】管理情報記憶機能１４は、ユーザ４ａから暗号化キーを受け付けた場合に、非公開暗号化キー１９を用いてユーザ４ａのユーザ名とユーザ４ａから受け付けた暗号化キーとを暗号化する。

【００３８】そして、管理情報記憶機能１４は、非公開暗号化キー１９を利用して暗号化されたユーザ名と暗号化キーとの組み合わせが新規の場合、記憶装置２１の暗号化キー管理情報２０に登録する。

【００３９】表1に、暗号化キー管理情報２０の一例を示す。なお、この表１では、暗号化キー管理情報２０の内容を説明容易とするために、ユーザ名と暗号化キーとが非公開暗号化キー１９で暗号化されていない状態を示しているが、実際は非公開暗号化キー１９でユーザ名と暗号化キーとが暗号化された状態で登録される。

【００４０】これにより、たとえデータベース管理者などが暗号化キー管理情報２０をアクセスしたとしても、どのユーザがどのような暗号化キーを利用しているか把握することができない。

【００４１】

【表１】

表１．暗号化キー管理情報（暗号化されていない状態）

ユーザ名	暗号化キー
ｕｓｅｒ１	ｋｅｙ
ｕｓｅｒ２	ｒｔ９ｋｅｕｔ３３３ｅ
ｕｓｅｒ３	ｄｉｔｏｕｔｅ８
ｕｓｅｒ１	ｄｊｔｉｅｏｔｊ４ｉｔｏｅａｔｕｅ
⋮	⋮

【００４２】判定機能１５は、ユーザ４ａから暗号化キーを受け付けた場合に、非公開暗号化キー１９を利用してユーザ４ａのユーザ名を暗号化し、この暗号化されたユーザ名に関する暗号化キー管理情報２０の登録件数をチェックする。

※【００４３】そして、判定機能１５は、登録件数が所定数以上の場合にアクセスを禁止する。

【００４４】図2は、登録要求変換機能１０による登録要求の変換状態の一例を示す図である。

【００４５】登録要求２２は、例えばＳＱＬで記述され

る。登録要求２２は、データベース２に格納されているテーブルTに、名前「ABC」、給料「1000」を登録することを要求する命令である。

【００４６】名前「ABC」及び給料「1000」は、機密事項のデータである。

【００４７】登録要求変換機能１０は、登録要求２２と暗号化キー「key」とを受け付けると、名前「ABC」及び給料「1000」を暗号化アルゴリズムfと暗号化キー「key」を利用して暗号化し、「dy1286」及び「ax57814」を得る。

【００４８】そして、登録要求変換機能１０は、名前「ABC」及び給料「1000」の代わりに「dy1286」及び「ax57814」を含む変換後の登録要求２３を求め、データ管理部３に発する。

【００４９】データ管理部３は、テーブルTの項目「名前」に「dy1286」、項目「給料」に「ax57814」を登録する。

【００５０】図３は、参照要求変換機能１１による参照要求の変換状態及びデータ復号化機能１２によるデータの復号化状態の一例を示す図である。

【００５１】参照要求２４は、例えばＳＱＬで記述される。参照要求２４は、「給料=1000」という条件を満たす「名前」及び「給料」の値を「テーブルT」から抽出するための命令である。

【００５２】条件に含まれている「1000」は、機密事項のデータに関する部分である。

【００５３】参照要求変換機能１１は、登録要求２４と暗号化キー「key」とを受け付けると、参照要求２４の条件に含まれている「1000」を暗号化アルゴリズムfと暗号化キー「key」を利用して暗号化し、「ax57814」を得る。

【００５４】そして、参照要求変換機能１１は、条件に含まれている「1000」の代わりに「ax57814」を含む変換後の参照要求２５を求め、データ管理部３に発する。

【００５５】データ管理部３は、テーブルTから項目「給料」の値が「ax57814」であるデータ２６を抽出する。

【００５６】データ復号化機能１２は、復号化アルゴリズムgと暗号化キー「key」を利用し、抽出されたデータ２６を復号化したデータ２７を求める。データ２７の内容は、「ABC,1000」となる。

【００５７】図４は、本実施の形態に係るアクセス管理プログラム７及びアクセス管理システム５によって実施されるアクセス管理方法の一例を示すフローチャートである。この図４に示す処理は、主に質問処理部１３の処理である。

【００５８】ステップＳ１では、ユーザ４ａから要求が受け付けられる。

【００５９】ステップＳ２では、受け付けた要求の種類が判定される。

【００６０】要求の種類がキー発行要求の場合には、ステップＳ３で暗号化キーが生成され、ステップＳ４でユーザ４ａに暗号化キーが返答される。

【００６１】要求の種類が登録要求又は参照要求の場合には、不正アクセス判定部１７による不正アクセスの判定処理が実行され、その後ステップＳ５で不正アクセスの判定結果がチェックされる。

【００６２】判定結果が「不正」の場合には、ステップＳ６が実行され、アクセスが禁止された旨がユーザ４ａに返答される。

【００６３】判定結果が「正当」の場合には、ステップＳ７が実行され、ユーザ４ａから受け付けた暗号化キーにより要求のデータ部が暗号化され、データベース管理システム１に提供される。

【００６４】データ部の暗号化された要求は、データベース管理システム１に受け付けられ、このデータ部の暗号化された要求に応じた処理がデータベース管理システム１によって実行される。

【００６５】ステップＳ８では、要求の種類が参照要求か否かが判定される。参照要求の場合には、ステップＳ９で参照されたデータが復号化され、ステップＳ１０で復号化されたデータがユーザ４ａに提供される。

【００６６】図５は、不正アクセス判定方法の一例を示すフローチャートである。この図５に示す処理は、主に不正アクセス判定部１７の処理である。

【００６７】ステップＴ１では、ユーザ名と暗号化キーとが受け付けられ、ステップＴ２では、受け付けられたユーザ名と暗号化キーとが非公開暗号化キー１９により暗号化される。

【００６８】ステップＴ３では、暗号化キー管理情報２０がアクセスされ、暗号化されたユーザ名と暗号化キーの組み合わせが暗号化キー管理情報２０に登録されていない新規の組み合わせか否かが判定される。

【００６９】判定の結果、新規の組み合わせの場合には、ステップＴ４で新規の組み合わせが暗号化キー管理情報２０に登録される。

【００７０】ステップＴ５では、ステップＴ１で受け付けられ非公開暗号化キー２０によって暗号化されたユーザ名を含む組み合わせが暗号化キー管理情報２０に何件登録されているか求められる。

【００７１】ステップＴ６では、求められた登録件数が所定数以上か否かが判定される。なお、この所定数は、異なる暗号化キーを受け付けたとしてもアクセスを許容する上限に基づいて予め設定される。

【００７２】判定の結果、登録件数が所定数以上の場合、ステップＴ７で「不正」が返答され、登録件数が所定数以上でない場合、ステップＴ８で「正当」が返答される。

【００７３】以上説明した本実施の形態においては、データベース２に暗号化されたデータが登録される。

【0074】そして、参照要求とともに適切な暗号化キーが受け付けられた場合にのみ、データベース2に登録されたデータの内容が把握できる。

【0075】暗号化キーは、データを登録したユーザのみしか持っていないため、たとえデータベース管理者や他のユーザがデータベース2をアクセスしたとしても、暗号化されたデータを復号化できない。

【0076】したがって、機密事項のデータを安全にデータベース2に保存することができる。例えば軍事機密、会社の機密、顧客情報、マーケティング情報の漏洩を防止できる。

【0077】なお、上記各実施の形態で説明した各構成要素は、自由に組み合わせてもよく、また複数の要素に分割してもよい。

【0078】また、本実施の形態におけるアクセス管理プログラム7は、複数のコンピュータ上に分散され、互いに連携しつつ動作してもよい。

【0079】また、アクセス管理プログラム7は通信媒体により伝送してコンピュータに適用可能である。アクセス管理プログラム7を読み込んだコンピュータは、アクセス管理プログラム7によって動作が制御され、上述した機能を実現する。

【0080】（第2の実施の形態）本実施の形態においては、上記第1の実施の形態に係るアクセス管理システム5及びアクセス管理プログラム7の具体的な利用態様について説明する。

【0081】図6は、アクセス管理システム5及びアクセス管理プログラム7の利用態様の一例を示すブロック図である。

【0082】データベース管理システム1とユーザ4aの操作するクライアント28とアクセス管理システム5とは、例えばインターネットなどのネットワーク29を介して接続されている。

【0083】データベース管理システム1は、データベース管理者30によって管理される。

【0084】アクセス管理システム5は、アクセス管理サービスを実施するサービス提供者31によって運営される。

【0085】データベース管理システム1の管理するデータベース2は、複数のユーザによって共用されるデータベースである。

【0086】クライアント28は、ユーザ4aの機密事項のデータをデータベース2に登録する場合に、アクセス管理システム5から固有の暗号化キー18を受信し、この暗号化キー18と登録要求とをアクセス管理システム5に送信する。

【0087】アクセス管理システム5は、暗号化キー18を利用して変換後の登録要求を求め、データベース管理システム1に送信する。これにより、データベース2に暗号化されたデータが登録される。

【0088】例えば、データベース管理者30や他のユーザがデータベース2のデータを参照しても、暗号化されているためその内容を把握することはできない。

【0089】クライアント28は、データベース2のデータを参照する場合、ユーザ4aに発行された暗号化キー18とともに参照要求をアクセス管理システム5に送信する。

【0090】アクセス管理システム5は、暗号化キー18を利用して変換後の参照要求を求め、データベース管理システム1に送信する。これにより、暗号化されたデータがデータベース2から読み出される。読み出されたデータは、アクセス管理システム5によって復号化され、クライアント28に送信される。

【0091】ユーザ4aは、機密事項のデータを安全にデータベース2に登録することができる。また、ユーザ4aは、サービス提供者31のアクセス管理サービスの提供を受けることで、自己でアクセスを管理するためのプログラムを保守、運用する必要がなく、効率的にアクセスを管理できる。

【0092】一方、サービス提供者31は、ユーザ4aからサービス料を得ることができる。

【0093】なお、アクセス管理プログラム7をクライアント28にダウンロードするためのサーバをアクセス管理システム5の代わりに設置し、このサーバをサービス提供者31が運営するとしてもよい。この場合、クライアント28で登録要求及び参照要求の変換が実行され、変換後の登録要求及び変換後の参照要求がクライアント28からネットワーク29を経由してデータベース2に送信される。データベース2から読み出されたデータは、クライアント28上で動作するアクセス管理プログラム7によって復号化される。

【0094】

【発明の効果】以上詳記したように本発明においては、アクセス要求側に対して暗号化キーが発行され、暗号化キーとともに登録要求が受け付けられると、この暗号化キーを利用して暗号化されたデータがデータベースに登録される。

【0095】また、暗号化キーとともに参照要求が受け付けられると、この暗号化キーを利用してデータベースに登録されている暗号化されたデータが参照され、参照されたデータが復号化される。

【0096】本発明では、アクセス要求側に発行された暗号化キーがこの発行を受けたアクセス要求側のみに保持される。これにより、他のアクセス要求側からデータベースが不正にアクセスされたとしても、データの機密性を確保できる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係るアクセス管理プログラム及びアクセス管理システムの一例を示すブロック図。

11

【図2】登録要求変換機能による登録要求の変換状態の一例を示す図

【図3】参照要求変換機能による参照要求の変換状態及びデータ復号化機能によるデータの復号化状態の一例を示す図。

【図4】同実施の形態に係るアクセス管理プログラム及びアクセス管理システムによって実施されるアクセス管理方法の一例を示すフローチャート。

【図5】不正アクセス判定方法の一例を示すフローチャート。

【図6】本発明の第2の実施の形態に係るアクセス管理システム及びアクセス管理プログラムの利用態様の一例を示すブロック図。

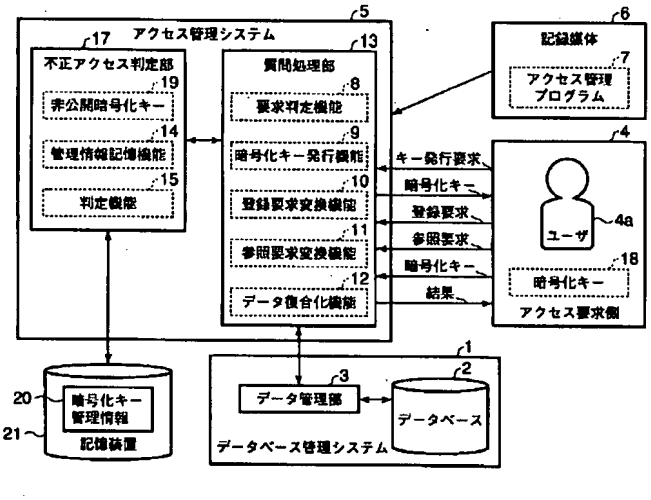
【符号の説明】

1…データベース管理システム
2…データベース
3…データ管理部

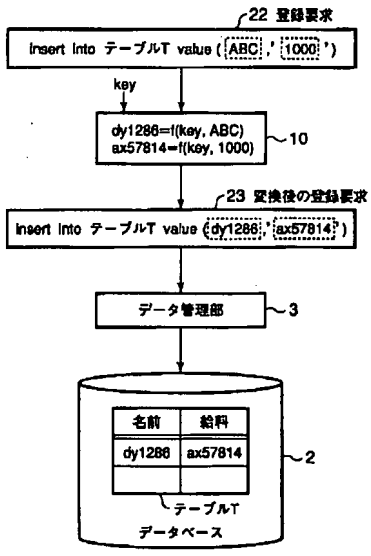
12

4…アクセス要求側
4a…ユーザ
5…アクセス管理システム
6…記録媒体
7…アクセス管理プログラム
8…要求判定機能
9…暗号化キー発行機能
10…登録要求変換機能
11…参照要求変換機能
12…データ復号化機能
13…質問処理部
14…管理情報記憶機能
15…判定機能
17…不正アクセス判定部
18…暗号化キー
19…非公開暗号化キー
20…暗号化キー管理情報
21…記憶装置
22…登録要求
23…変換後の登録要求

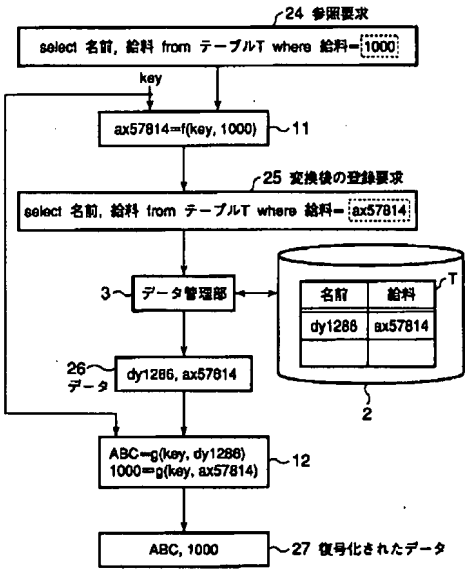
【図1】



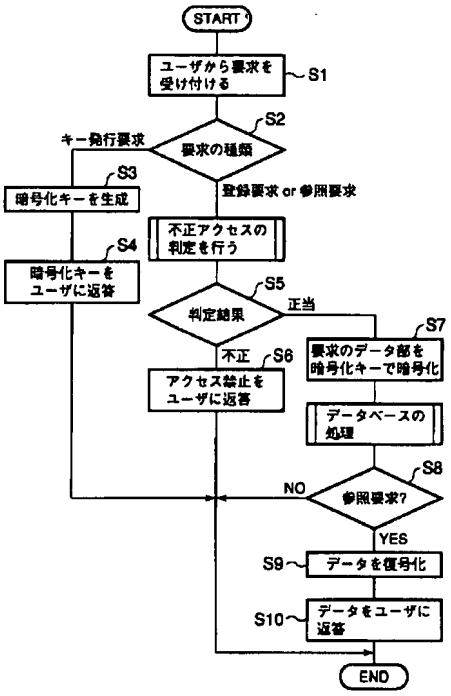
【図2】



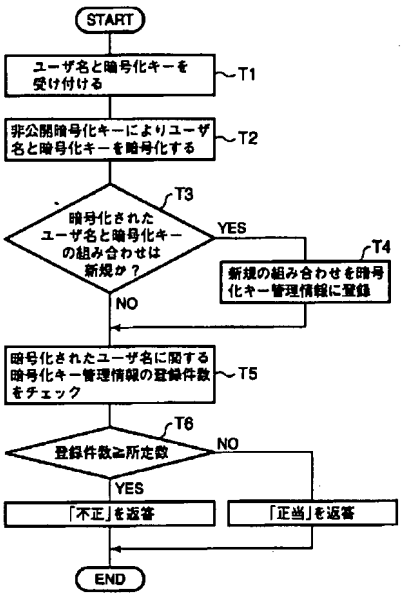
【図3】


24 参照要求
select 名前, 給料 from テーブルT where 給料=1000
key
ax57814=f(key, 1000)
11
25 変換後の登録要求
select 名前, 給料 from テーブルT where 給料= ax57814
3
データ管理部
名前
給料
dy1288
ax57814
T
2
26
データ
dy1286, ax57814
ABC=g(key, dy1286)
1000=g(key, ax57814)
12
ABC, 1000
27 復号化されたデータ

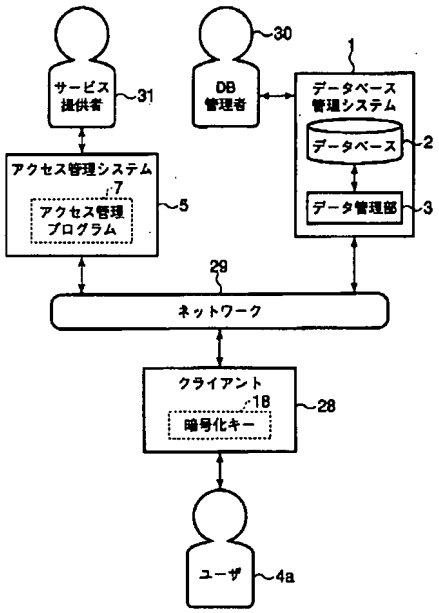
【図4】


START
ユーザから要求を受け付ける
S1
S2
要求の種類
キー発行要求
S3
暗号化キーを生成
S4
暗号化キーをユーザに返答
登録要求 or 参照要求
不正アクセスの判定を行う
S5
判定結果
正当
S7
要求のデータ部を暗号化キーで暗号化
不正
S6
アクセス禁止をユーザに返答
データベースの処理
S8
参照要求?
NO
YES
S9
データを復号化
S10
データをユーザに返答
END

【図5】


START
ユーザ名と暗号化キーを受け付ける
T1
非公開暗号化キーによりユーザ名と暗号化キーを暗号化する
T2
T3
暗号化されたユーザ名と暗号化キーの組み合わせは新規か？
YES
T4
新規の組み合わせを暗号化キー管理情報に登録
NO
暗号化されたユーザ名に関する暗号化キー管理情報の登録件数をチェック
T5
T6
登録件数≧所定数
NO
YES
「不正」を返答
「正当」を返答
END

【図6】


サービス提供者
31
DB管理者
30
1
データベース管理システム
データベース
2
データ管理部
3
アクセス管理システム
7
アクセス管理プログラム
5
29
ネットワーク
クライアント
18
暗号化キー
28
ユーザ
4a

フロントページの続き

Fターム(参考) 5B017 AA03 AA07 BA06 BA07 CA16
5B075 KK43
5B082 EA11 GA11
5J104 AA16 EA16 NA02 NA06 NA27
PA07